AO 106 (Rev. 04/10) Application for a Search Warrant

AUTHORIZED AND APPROVED/DATE: MATTHEW DILLON

Digitally signed by MATTHEW DILLON
Date: 2022.08.06 11:22:26 -05'00'

UNITED STATES DISTRICT COURT

for the

Western District of Oklahoma

In the Matter of the Search of

415 Webster Dr., Wayne, Oklahoma 73096; 2014 Metallic-Brown Chevy Siverado, Oklahoma Tag CN13711, VIN # 1GCVKREC0EZ153231; and White and Blue Harley-Davidson Motorcycle, Oklahoma Tag K2532

Case No. M-22-560 STE

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A"

located in the Western District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment "B" which is incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 875(c)	Transmitting a communication containing a threat to injure another in interstate commerce

The application is based on these facts:

See attached Affidavit of FBI Special Agent Audra Rees, which is incorporated by reference herein.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Audra Rees, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: August 6, 2022

Judge's signature

City and state: Lawton, OK

SHON T. ERWIN, U.S. MAGISTRATE JUDGE

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Audra Rees, Special Agent with the Federal Bureau of Investigation, being duly sworn, hereby depose and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) Joint Terrorism Task Force (JTTF). I have been employed as a Special Agent with the FBI since 2020, and I am currently assigned to the Oklahoma City Division. I have participated in investigations involving individuals suspected of terrorist activities, assisted in the execution of search and arrest warrants, conducted surveillance, analyzed records, and have spoken to informants and subjects of investigations involving numerous types of federal violations including firearms related offenses.

2. I have personally participated in the investigation set forth below. The facts in this Affidavit come from my personal observations, my review of documents related to this investigation, oral and written communications with others who have personal knowledge of the events and circumstances described herein, a review of public source information including information available on the Internet, my training and experience, and information obtained from other agents and witnesses. This Affidavit is intended to show there is sufficient probable cause for the requested warrant, but it does not set forth all of my knowledge about this matter.

3. This affidavit is made in support of an application for a warrant to search the residence of Charles Dean Lack, (hereafter **LACK**), 415 Webster Dr., Wayne, Oklahoma

73096, a 2014 Metallic-Brown Chevy Silverado, Oklahoma tag CN13711, VIN # 1GCVKREC0EX153231, and a White and Blue Harley-Davidson motorcycle, Oklahoma tag K2532 (hereafter referred to as the SUBJECT PREMISES) in the Western District of Oklahoma (more particularly described in Attachment A), and seize evidence related to a violation of 18 U.S.C. § 875 (Threat via interstate communication).

4. Title 18, United States Code, Section 875 (c) defines a threat via interstate communication as whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another.

5. On or about August 5th, 2022, the FBI electronically received a tip via the FBI's National Threat Operations Center (NTOC) in Clarksburg, West Virginia, from an individual who identified themselves as Charles Dean Lack submitted their information as:

First Name: Dean
Middle Name:
Last Name: Lack
DOB: XX/XX/1966[1]
Phone Type: Cell
International: False
Phone Number: 4053177491
Phone Ext:
Email: deanlack55@aol.com
Type: Residential
Address: 415 webster dr.
City: Wayne
State: OK
Zip: 73096
Additional Info:

[1] **LACK** provided his full date of birth, which has been redacted in this affidavit.

The text the individual submitted is as follows:

> "I'm Charles Dean Lack retired as an Oklahoma City police officer /pilot I'm fixing to head to will Rogers airport in okc to start killing every homeland security's employees for being corrupt and illegally holding my future wife in custody I have all the proof and willing to give my life for her if it takes in killing everyone that is involved in this corrupt world of government employees I don't care if my life gets taken because several will go before I do, I turned this in to the FBI several months ago and nothing has been done so I feel like I should go solve this problem to get my future wife to get where she belongs and it's not with homeland security at the airport. I'm not drunk and on no drugs I'm very healthy and capeable of making everything happen even willing to let anyone try to stop me from stopping illegal homeland security guards to keep breaking the law. Enough is enough."

6. The individual that made the tip listed a victim of a crime, R.R.[2], provided a date of birth, and listed the address as "California, CA." The individual, based on a previous tip, seems to believe that Homeland Security at the Will Rodgers World Airport (WRWA) is holding R.R. against her will. According to open-source information, R.R. is a famous MMA fighter. She is currently married to another famous MMA fighter and they live in California.

7. The threat that was submitted on August 5, 2022, caused great concern to WRWA officials. The Assistant Federal Security Director (AFSD) stated, in regards to whether or not this was perceived as a true threat, said "absolutely." The AFSD was concerned specifically because of **LACK**'s knowledge of aviation, airport layout, police tactics, and weapons training. **LACK** is a retired police officer who is also a trained pilot.

[2] **LACK** provided the first and last name, but it has been redacted to the first name and last name initials in this affidavit.

8. The IP address that submitted the tip was captured. The Internet Service Provider (ISP) provided FBI with information that the registered user of the IP address is Dean Lack. The Service Address is 415 Webster Dr, Wayne, OK 73095, telephone number 405-449-3107. The billing address is PO Box 268, Wayne, OK 73095, and an alternate telephone number is listed as 205-317-7491. This IP address was started July 13, 2022, at 01:00:23 CST and was current to the EDR on August 5, 2022, at 18:01:55 CST.

9. On June 23, 2022, **LACK** submitted a tip to NTOC that included the same user information (name, DOB, cell phone number, address). The IP address used was different at the time. The following text was submitted in regards to the tip:

> "She is my future wife flew in from California and tge [sic] homeland security has corrupt her and I they will not release her to her freedom they keep her as a hostage in the airport in Oklahoma City she needs the FBI to get her out of there and don't try to get her to pay any fee or anything until the FBI does their job and don't be a corrupt idiot get her out of there before there is murder starts going on there to stop the homeland security corrupt idiots to keep doing this and I have sent this 3 : times now so just get to doing your damn job or come get me and put me in prison where I will start taking matters into my own hands is what they need anyway."

10. In connection with the incident on June 23, 2022, local police made contact with **LACK**. **LACK** told the officer that arrived that **LACK** had recent health issues. **LACK** told the officers that R.R. was coming to visit him, but that she got detained at the airport by Homeland Security at the airport. **LACK** denied being involved in a monetary scam.

11. On or about August 6, 2022, FBI made contact with **LACK** at his residence, the SUBJECT PREMESIS. **LACK** was Mirandized, stated that he knew his rights, and answered questions. **LACK** stated that he has been talking with who he believes to be R.R. for some time now. They used to communicate through Google Hangouts and now communicate via Telegram. R.R. calls **LACK** once a day. They have never video-chatted. **LACK** stated R.R. is being held against her will at the WRWA. **LACK** admitted to making the threat but stated he did not intend to carry it out. **LACK** said that no one would do anything about his concerns until he threatened to go to the airport and kill HSI agents. **LACK** visited the airport on 3 separate occasions to determine where HSI is in the airport. **LACK** intended the statement submitted to NTOC to be taken as a threat. **LACK** knew it would likely be taken as a threat. **LACK** made the threat to get the attention of various officials. **LACK** saw how much attention recent mass shootings have garnered and wanted to gain attention. Besides R.R., **LACK** said that he had a strange interaction with a person he believed to be Christopher Wray, who **LACK** is fairly certain is an FBI Agent.[3] "Wray" asked **LACK** to send Wray $700, then Wray promised to send **LACK** 7 million dollars. **LACK** denied sending money to Wray. **LACK** did send money to R.R. **LACK** thinks it is around $1200 **LACK** sent to R.R. so far. **LACK** denied that he had no lasting brain injury from previous motorcycle wreck.

[3] Christopher Wray is the Director of the FBI.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

12. Based on the above evidence, **LACK** used an electronic device to make the threat. Based on my training and experience, I am aware that persons involved in such activities will typically keep the instrumentalities of their crime, including but not limited to the electronic devices, to include computers and cellular telephones, used in the commission of the aforementioned offenses in their residences. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on electronic devices or a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure and subsequent search of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

13. I submit that if a computer or other electronic storage medium, such as a smartphone or computer, is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be

recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

Forensic Evidence

14. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage devices, including electronic storage media, may provide

crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers and electronic devices typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.

Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Lastly, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer or an electronic device works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer or an electronic device is evidence may depend on other information stored on the computer and the application of knowledge about how a computer or an electronic device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer or an electronic device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

Necessity of Seizing or Copying Entire Computers or Storage Media

15. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors

and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and

reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

Nature of Examination

16. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant. In addition, this warrant seeks permission to transport seized electronics from the SUBJECT PREMISES to districts outside of the Western District of Oklahoma for forensic analysis and extraction as necessary.

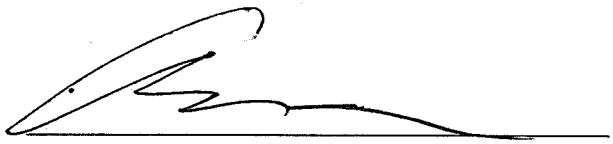
CONCLUSION

17. Based on the facts presented above, there is probable cause to believe that **LACK** knowingly made a threat via interstate communications in violation of Title 18, Section 875.

18. Accordingly, I respectfully request that the Court issue a search warrant for the SUBJECT PREMISES (more particularly described in Attachment A and seize items

permission to search for firearms, firearm parts, ammunition, records related to the purchase of the aforementioned items, and records and evidence related to any coconspirators.

Respectfully submitted,



Audra Rees
Special Agent
Federal Bureau of Investigation

Signed before me on this 6th day of August, 2022.

Shon T. Erwin

JUDGE **SHON T. ERWIN**
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PREMISES TO BE SEARCHED

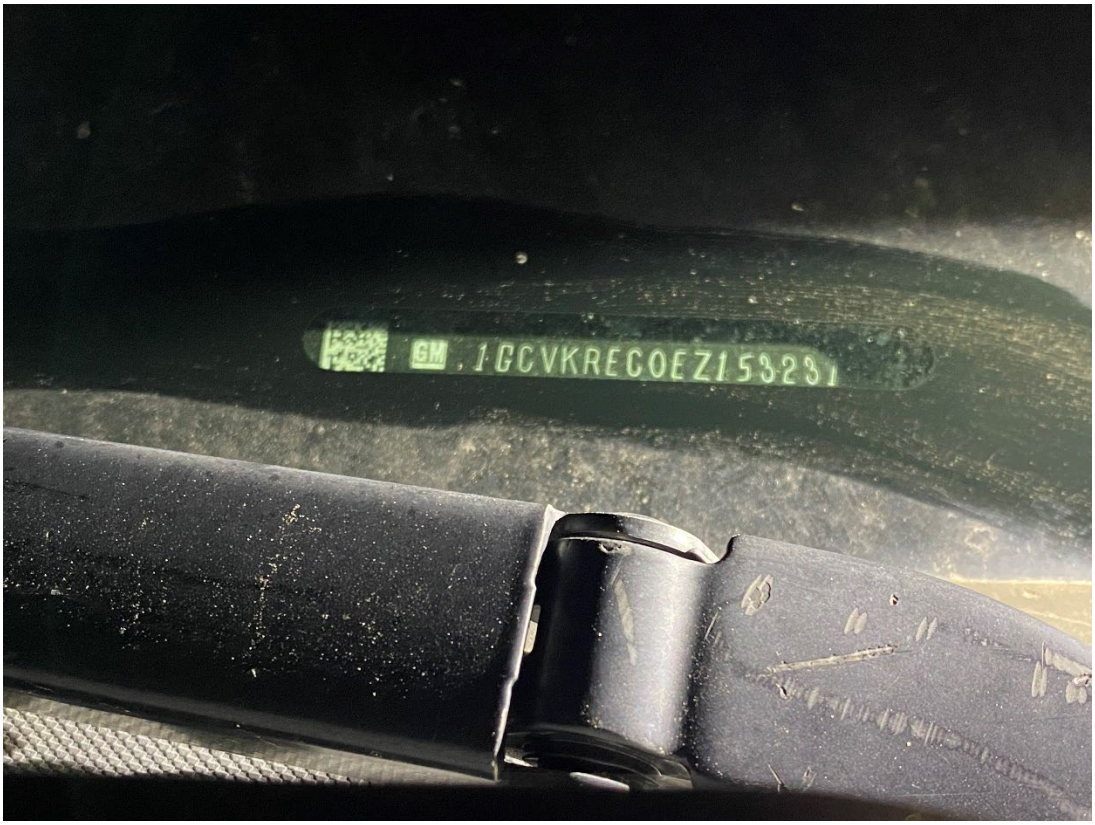
ATTACHMENT A

PREMISES TO BE SEARCHED

The property to be searched is 415 Webster Dr, Wayne, OK, a 2014 Metallic-Brown Chevy Silverado, Oklahoma tag CN13711, VIN # 1GCVKREC0EX153231, and a White and Blue Harley-Davidson motorcycle, Oklahoma tag K2532, in its entirety, including any outbuildings. The residence is a one bed, one bath apartment part of a larger apartment complex. This complex is a one story, brown brick structure with a metal roof. The windows and doors have a white trim. Apartment 415 has a sign with the numeric on the outside of the building.


455


4X4
SILVERADO


GM 1GCVKRECOEZ153231


06 ML
MCCLAIN
OKLAHOMA
K2532
THE CHICKASAW NATION

ATTACHMENT B

Property to be Seized

1. There is probable cause to seize the following items, which constitute evidence of a violation of Title 18, United States Code, Sections 875, found at the SUBJECT PREMISES:

a. Any digital device used to facilitate the above-listed violations and forensic copies thereof;

b. Any firearm, firearm part, or ammunition;

c. Any record or document pertaining to the possession or acquisition of any weapon, including firearms;

d. Any record or document, including diaries, books, notebooks, notes, computer printouts, drawings, photographs, video recordings, and any other records related to firearms;

e. Any records or document reflecting or related to any intent, motive, or means of committing the violations listed above;

f. Records and information relating to any social media account utilized by Charles Dean Lack;

g. Any documents, records, programs, or applications tending to demonstrate the actual user(s) of computers found at the SUBJECT PREMISES. As used above, the terms records, documents, programs, applications, or materials include records, documents, programs, applications or materials created, modified or stored in any form;

h. Evidence of the motive, opportunity, intent, preparation, plan, knowledge, identity, absence of mistake, willingness, state of mind, or accident related to threats to injure or kill another. This specifically includes the electronic devices, computers, wireless phones, digital cameras, and other items and areas listed in this Attachment and Warrant;

and

i. Evidence of others who aided and abetted, counseled, commanded, or induced, the communication of threats to injure or kill another. This specifically includes the electronic devices, computers, wireless phones, digital cameras and other items and areas listed in this Attachment and Warrant.

2) Any computers, tablets, mobile phones, associated storage devices, other devices located therein that can be used to store information and/or connect to the Internet, and/or records and materials.

3) Evidence identifying the individual(s) who used, owned, or controlled the computer(s) and cellular devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, accounts of Internet Service Providers.

4) For any computer, computer hard drive, cellular phone, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that may contain things otherwise called for by this warrant:

a. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

b. evidence of the lack of such malicious software;

c. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

e. evidence of the times the COMPUTER was used;

f. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

g. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

h. contextual information necessary to understand the evidence described in this attachment.

5) As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

6) The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

7) The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

8) This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.